1. A method for combining multiple access points and utilizing a certificate as an access method to a host system from one of a plurality of access points, comprising:

creating and distributing a certificate for certificate-based authentication to any one of a plurality of storage methods selected from a group of storage methods consisting of at least a microcomputer of an integrated chip card, a disk of a computer disposed in a secure environment, and a hardware security module (HSW) associated with a computer;

managing the certificate over a life span of the certificate at least in part via a lightweight directory assistance protocol (LDAP) directory shared by a certificate authority (CA) and a card life cycle management system (CCLCMS); and

allowing access to the host system using the certificate for public key-based authentication to an application on a host server.

2. The method of claim 1, wherein creating and distributing the certificate further comprises creating and distributing the certificate for storage on the microcomputer of the integrated chip card.

3. The method of claim 2, wherein creating and distributing the certificate for storage on the microcomputer of the integrated chip card further comprises preparing a key pair for the card and placing a unique PIN on the card by an initialization workstation.

4. The method of claim 3, wherein creating and distributing the certificate for storage on the microcomputer of the integrated chip card further comprises creating and signing the certificate by the CA in response to a request for the certificate received via a registration authority (RA).

5. The method of claim 4, wherein creating and distributing the certificate for storage on the microcomputer of the integrated chip card further comprises posting a copy of the certificate to the LDAP directory shared by the CA and the CCLCMS in a location in which log-in rights and access rights for a holder of the card are identified to the CLCMS.

6. The method of claim 5, wherein creating and distributing the certificate for storage on the microcomputer of the integrated chip card further comprises distributing the card and PIN to the cardholder through separate channels for security.

7. The method of claim 1, wherein creating and distributing the certificate further comprises creating and distributing the certificate for storage on the disk of the

computer disposed in the secure environment by creating the certificate via a badging station that interacts with the CCLCMS and which stores an encrypted private key for the certificate on a computer disk at the badging station.

8. The method of claim 7, wherein creating and distributing the certificate for storage on the disk of the computer disposed in the secure environment further comprises allowing a user on an external system to request the certificate via the badging station and sending the user's request to the CA via a registration authority (RA) for creation of the certificate.

9. The method of claim 8, wherein creating and distributing the certificate for storage on the disk of the computer disposed in the secure environment further comprises creating the certificate by the CA and posting the certificate to the LDAP directory shared by the CA and the CCLCMS.

10. The method of claim 9, wherein creating and distributing the certificate for storage on the disk of the computer disposed in the secure environment further comprises sending an email notice of the certificate to the user and allowing downloading and storage of the certificate in response to a request by the user.

11. The method of claim 1, wherein creating and distributing the certificate further comprises creating and distributing the certificate for storage on the HSW by creating a key pair by the HSM in response to a request for a user, storing a private key of the key pair on the HSM, and delivering only a public key of the key pair external to the HSM.

12. The method of claim 11, wherein creating and distributing the certificate for storage on the HSW further comprises creating an entry in the LDAP for the user and sending the request to the CA by a registration authority (RA).

13. The method of claim 12, wherein creating and distributing the certificate for storage on the HSW further comprises receiving the request by the CA, verifying that the request is complete, creating the certificate, and sending an email to the user confirming creation of the certificate

14. The method of claim 13, wherein creating and distributing the certificate for storage on the HSW further comprises allowing download and storage of the certificate, including only the public key, on a computer disk for the user.

15. The method of claim 1, wherein managing the certificate over the life span of the certificate further comprises at least one of re-issuing the certificate in response to a request received upon notification of an approaching expiry for the certificate,

sending notification of the approaching expiry for the certificate, issuing a new certificate in response to a request upon expiry of the certificate, revoking the certificate according to pre-defined parameters and simultaneously removing information regarding the revoked certificate from a user access definition within the LDAP directory shared by the CA and the CCLCMS.

16. The method of claim 1, wherein allowing access to the host system using the certificate for public key-based authentication further comprises allowing the user to utilize the certificate stored within the microcomputer of the integrated chip card to access the application on the host server, such that when the user accesses the application on the server, the application requires that the card and certificate are present for authentication of the user.

17. The method of claim 1, wherein allowing access to the host system using the certificate for public key-based authentication further comprises allowing an external system to access the application on the host server utilizing the certificate and associated keys stored on a disk of the computer of the external system for authentication of itself to the host server.

18. The method of claim 1, wherein allowing access to the host system using the certificate for public key-based authentication further comprises allowing an external system to access the application on the host server utilizing the certificate and associated keys stored on the HSW which stores encryption keys and encrypts information passed into it and passes the encrypted information out of it and that is associated with a computer of the external system for authentication of itself to the host server.

19. A system for combining multiple access points and utilizing a certificate as an access method to a host system from one of a plurality of access points, comprising:

means for creating and distributing a certificate for certificate-based authentication to any one of a plurality of storage methods selected from a group of storage methods consisting of at least a microcomputer of an integrated chip card, a disk of a computer disposed in a secure environment, and a hardware security module (HSW) associated with a computer;

means for managing the certificate over a life span of the certificate at least in part via a lightweight directory assistance protocol (LDAP) directory shared by a certificate authority (CA) and a card life cycle management system (CCLCMS); and

means for allowing access to the host system using the certificate for public key-based authentication to an application on a host server.